



## DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets <sup>6</sup> :  
G07F 7/10

A1

(11) Numéro de publication internationale: WO 96/32701

(43) Date de publication internationale: 17 octobre 1996 (17.10.96)

(21) Numéro de la demande internationale: PCT/FR96/00500

(22) Date de dépôt international: 3 avril 1996 (03.04.96)

(30) Données relatives à la priorité:  
95/04533 14 avril 1995 (14.04.95) FR

(71) Déposant: G C TECH [FR/FR]; 16, place Vendôme, F-75001 Paris (FR).

(72) Inventeurs: PAYS, Paul-André; 34, rue Juliette-Adam, F-91190 Gif-sur-Yvette (FR). BEN DAHAN, Gérard; 5, rue d'Alsace, F-75010 Paris (FR).

(74) Mandataires: JOLY, Jean-Jacques etc.; Cabinet Beau-de-Loménie, 158, rue de l'Université, F-75007 Paris (FR).

(81) Etats désignés: AU, BR, CA, CN, HU, JP, KR, MX, RU, SG, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

## Publiée

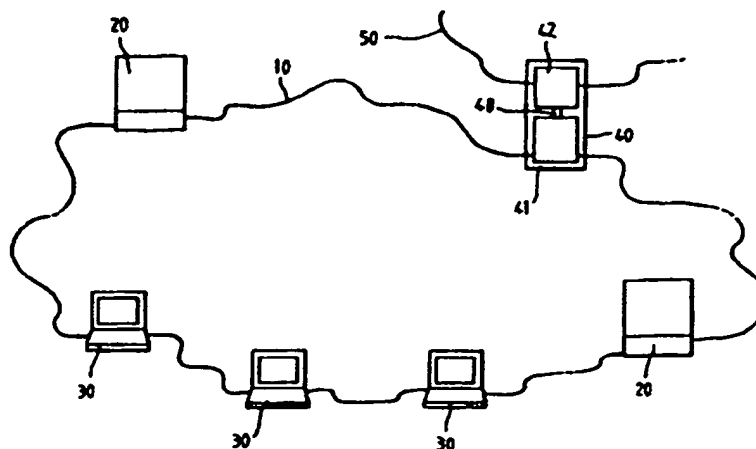
*Avec rapport de recherche internationale.  
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si de telles modifications sont reçues.*

(54) Title: ELECTRONIC PAYMENT METHOD FOR PURCHASE-RELATED TRANSACTIONS OVER A COMPUTER NETWORK

(54) Titre: PROCEDE DE PAIEMENT ELECTRONIQUE PERMETTANT D'EFFECTUER DES TRANSACTIONS LIEES A L'ACHAT DE BIENS SUR UN RESEAU INFORMATIQUE

## (57) Abstract

A method using an open communication network (10) to which retailer server stations (20) and customer stations (30) are connected. According to the method, a retailer server station generates a payment slip for the planned purchase transaction between the retailer and a customer, which slip comprises data on the retailer, the customer, the purchased item or service and the price; the payment slip is transmitted over the network to a payment server station (40); the payment server automatically checks whether the payment of said price is authorised for the customer in question, by querying the client's personal account set up in the payment server for paying small amounts, or, in the case of larger amounts, by making a query over a banking network (50) separate from the computer network (10); if the payment is authorised, the payment server generates a cash voucher comprising at least some of the data on the payment slip; and the cash voucher is transmitted to the retailer to enable the purchase to go ahead.



(57) Abrégé

Le procédé utilise un réseau de communication ouvert (10) sur lequel sont connectés des postes serveurs de marchands (20) et des postes clients (30) et comprend: l'élaboration par un poste serveur de marchand d'un ticket de paiement, concernant un achat envisagé entre le marchand et un client, et comportant des informations relatives au marchand, au client, à l'objet de l'achat et à son prix; la transmission du ticket de paiement via le réseau à un poste serveur de paiement (40); la vérification automatique par le serveur de paiement si le paiement du prix est autorisé pour le client concerné, soit par interrogation d'un compte client propre au client, tenu par le serveur de paiement, et destiné au paiement des petits montants, soit par interrogation sur un réseau bancaire (50) indépendant du réseau informatique (10), pour les paiements de montants plus élevés; si la vérification est positive, l'élaboration par le serveur de paiement d'un bon de caisse comportant au moins une partie des informations du ticket de paiement; et la transmission du bon de caisse au serveur de marchand afin d'autoriser la réalisation de l'achat.

**UNIQUEMENT A TITRE D'INFORMATION**

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AT	Arménie	GB	Royaume-Uni	MW	Malawi
AT	Autriche	GE	Géorgie	MX	Mexique
AU	Australie	GN	Guinée	NE	Niger
BB	Barbade	GR	Grèce	NL	Pays-Bas
BE	Belgique	HU	Hongrie	NO	Norvège
BF	Burkina Faso	IE	Irlande	NZ	Nouvelle-Zélande
BG	Bulgarie	IT	Italie	PL	Pologne
BJ	Bénin	JP	Japon	PT	Portugal
BR	Brésil	KE	Kenya	RO	Roumanie
BY	Bélarus	KG	Kirghizistan	RU	Fédération de Russie
CA	Canada	KP	République populaire démocratique de Corée	SD	Soudan
CF	République centrafricaine	KR	République de Corée	SE	Suède
CG	Congo	KZ	Kazakhstan	SG	Singapour
CH	Suisse	LI	Liechtenstein	SI	Slovénie
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovaquie
CM	Cameroun	LR	Libéria	SN	Sénégal
CN	Chine	LT	Lituanie	SZ	Swaziland
CS	Tchécoslovaquie	LU	Luxembourg	TD	Tchad
CZ	République tchèque	LV	Lettonie	TG	Togo
DE	Allemagne	MC	Monaco	TJ	Tadjikistan
DK	Danemark	MD	République de Moldova	TT	Trinité-et-Tobago
EE	Estonie	MG	Madagascar	UA	Ukraine
ES	Espagne	ML	Mali	UG	Ouganda
FI	Finlande	MN	Mongolie	US	Etats-Unis d'Amérique
FR	France	MR	Mauritanie	UZ	Ouzbékistan
GA	Gabon			VN	Viet Nam

**Procédé de paiement électronique permettant d'effectuer des transactions liées  
à l'achat de biens sur un réseau informatique**

La présente invention concerne un procédé de paiement électronique  
5 permettant d'effectuer des transactions liées à l'achat de biens offerts par des  
marchands au moyen de services télématiques via un réseau de télécommunication  
informatique ouvert sur lequel sont connectés des postes serveurs de marchands et  
des postes clients.

Par réseau informatique ouvert, on entend ici un réseau sur lequel des  
10 particuliers ou des entreprises peuvent librement se connecter à la condition de  
disposer d'une adresse, par exemple le réseau "Internet". Les biens concernés sont  
des produits ou des services, dont la fourniture est réalisée hors du réseau après la  
conclusion de la transaction, ou des biens immatériels, tels que des informations,  
dont la fourniture peut être réalisée via le réseau informatique.

15 Divers procédés de paiement électronique ont été proposés, certains  
étant déjà opérationnels.

Plusieurs procédés sont fondés sur une nouvelle représentation de la  
monnaie. Il s'agit d'une représentation électronique, quelquefois dénommée "jeton"  
qui peut être purement logicielle ou partiellement matérielle, par exemple avec une  
20 carte à puce. Ces procédés impliquent la circulation de monnaie sur le réseau  
informatique, ce qui pose des problèmes difficiles de sécurité vis-à-vis de la  
création de fausse monnaie.

D'autres procédés connus de paiement électronique impliquent une  
relation directe avec une banque ou un réseau bancaire. Typiquement, de tels  
25 procédés sont employés dans les réseaux de carte de crédit comme, par exemple,  
des procédés bien connus utilisant des terminaux points de vente reliés à un circuit  
carte bancaire ainsi que des procédés utilisant des chèques électroniques avec une  
signature électronique pour l'authentification de l'acheteur. C'est une forme de  
lettre d'engagement émise par un acheteur, remise au vendeur et acceptée et  
30 reconnue par une banque.

Les procédés qui impliquent à un moment ou un autre de la transaction  
une relation avec le système bancaire traditionnel et la mise en oeuvre d'une  
transaction dans ce système présentent des inconvénients. Ainsi, les transactions  
dans le système bancaire ont un coût réel qui devient prohibitif lorsque le montant  
35 de l'achat est très faible, par exemple un montant associé à la consultation d'une  
base de données. Or, les réseaux informatiques sont bien adaptés à la vente de

biens de faible valeur, principalement des biens d'information, puisque la livraison du bien peut se faire par le réseau lui-même. En outre, l'accès à un réseau bancaire ou un réseau de carte bancaire doit être hautement protégé, ce qui exclut pratiquement la possibilité d'un accès à travers un réseau informatique ouvert, tel que le réseau "Internet" sur lequel des acheteurs potentiels peuvent se connecter.

L'invention a pour but de fournir un procédé permettant d'éviter les inconvénients des procédés connus, en particulier un procédé permettant, sans circulation de monnaie électronique, de réaliser de façon simple et fiable des transactions liées à l'achat de biens sur un réseau informatique, et ce aussi bien pour des biens de prix élevé nécessitant une autorisation par le système bancaire traditionnel, que pour des biens de faible ou très faible prix.

Ce but est atteint grâce à un procédé du type défini en tête de la présente description et comportant, conformément à l'invention, les étapes de :

– élaboration par un poste serveur de marchand connecté au réseau d'une demande d'autorisation de transaction, ou "ticket de paiement", concernant un achat envisagé entre le marchand et un client, et comportant des informations relatives au marchand, au client, à l'objet de l'achat et à son prix,

– transmission du ticket de paiement via le réseau informatique à un poste serveur de paiement distinct des postes clients et serveurs de marchands,

– vérification automatique par le serveur de paiement si le paiement du prix est autorisé pour le client concerné, la vérification étant effectuée, selon le montant du prix à payer, soit par interrogation d'un compte propre au client, tenu par le serveur de paiement, et destiné au paiement des petits montants, soit par interrogation sur un réseau bancaire indépendant du réseau informatique, pour les paiements de montants plus élevés,

– si la vérification est positive, élaboration par le serveur de paiement d'une autorisation de transaction ou bon de caisse comportant au moins une partie des informations du ticket de paiement, et

– transmission du bon de caisse au serveur de marchand via le réseau informatique, afin d'autoriser la réalisation de l'achat.

Ainsi, le procédé selon l'invention est remarquable en ce qu'il n'implique ni la création de monnaie électronique, ni la circulation de monnaie électronique sur le réseau informatique.

La gestion des transactions est effectuée par un serveur de paiement qui seul peut accéder à un réseau bancaire ou un réseau de carte bancaire, et qui

gère des comptes clients non bancaires sur lesquels des transactions de faibles montants peuvent être effectuées.

Le serveur de paiement gère également des comptes marchands non bancaires utilisés pour les transactions de faibles montants. Ainsi, lorsqu'un bon de  
5 caisse est transmis après vérification par interrogation d'un compte client tenu par le serveur de paiement, le montant de l'achat est débité du compte client et crédité sur un compte marchand propre au marchand concerné et tenu par le serveur de paiement, ce qui n'entraîne pas des coûts de traitement élevés.

Chaque client dispose d'une identité qui lui est propre pour pouvoir  
10 utiliser le procédé de paiement. Il doit également disposer d'un compte bancaire réel, de préférence un compte utilisable au moyen du système traditionnel des cartes bancaires. La vérification par le serveur de paiement peut comprendre une phase préalable de validation de l'identité du client à partir du contenu du ticket de paiement. La validation de l'identité est une opération préalable à l'accès éventuel  
15 au compte du client, si le montant de l'achat est faible, et/ou à l'accès au réseau bancaire si le montant est plus élevé. Le serveur de paiement comporte de préférence des moyens, par exemple une base de données, permettant de mémoriser les relations entre les identités des clients utilisées pour les transactions sur le réseau informatique et des identités bancaires (numéros de comptes  
20 bancaires ou numéros de cartes de crédit) utilisées pour les transactions sur le réseau bancaire. On peut éviter de la sorte la circulation d'identités bancaires sur le réseau informatique.

Un mode de réalisation de l'invention sera maintenant décrit à titre indicatif, mais non limitatif, en référence aux dessins annexés sur lesquels :

- 25
- la figure 1 est une vue générale très schématique d'un système de paiement électronique conforme à l'invention ;
  - la figure 2 est une représentation sous forme d'un schéma bloc d'un serveur de paiement du système de la figure 1 ;
  - la figure 3 illustre le déroulement des opérations relatives à un achat  
30 au moyen du système de la figure 1 ; et
  - les figures 4A à 4C sont des organigrammes montrant très schématiquement les opérations effectuées par le serveur de paiement.

Sur la figure 1 est représenté de façon très schématique un réseau de télécommunication informatique 10 sur lequel sont connectés des postes serveurs  
35 de marchands 20, des postes clients 30 et au moins un poste serveur de paiement 40.

Le réseau informatique 10 est un réseau ouvert ou public, par exemple le réseau dénommé "Internet".

Les serveurs de marchands 20 sont des unités telles que celles couramment utilisées pour des serveurs télématiques connectés sur "Internet", par exemple des unités organisées autour de machines "Unix" multiprocesseurs.

Les postes clients 30 sont essentiellement des micro-ordinateurs qui sont munis de moyens de connexion au réseau "Internet" 10, par exemple sous forme d'interface "Web". Les serveurs de marchands 20 et de postes clients 30 utilisent par exemple des logiciels connus sous la dénomination "World Wide Web" (WWW) utilisant le protocole HTTP.

Le serveur de paiement 40, montré avec plus de détails sur la figure 2, comprend des unités frontale et dorsale respectivement 41 et 42 connectées toutes les deux au réseau "Internet" 10. L'unité frontale 41 a une architecture semblable à celle d'un serveur classique connecté sur un réseau tel qu'"Internet". L'unité dorsale 42 comporte une unité de traitement 43 à un ou plusieurs processeurs, une base de données 44 comportant des informations relatives aux marchands et clients abonnés au système de paiement, un registre de transactions 45, une unité 46 d'interface avec un réseau bancaire ou un réseau de carte bancaire 50, et un bus de communication 47 ou autre liaison similaire permettant de relier entre eux les différents constituants de l'unité dorsale 42. Une liaison sécurisée 48 permet une communication bidirectionnelle entre l'unité frontale 41 et l'unité de traitement 43. La communication avec le réseau informatique 10 est contrôlée par l'unité frontale 41 tandis que la gestion de la base de données 44 ainsi que le contrôle de la communication avec le réseau bancaire 50 sont assurés par l'unité dorsale 42.

La base de données 44 contient des informations relatives aux clients et aux marchands abonnés au système de paiement. Pour chaque client, la base de données 44 contient l'identité système du client ("CId"), identité reçue lors de l'abonnement au système, un compte de client ou porte monnaie électronique ("PME") destiné au paiement de faibles montants, une identité bancaire telle que numéro de compte bancaire réel ou numéro de carte de crédit ainsi qu'éventuellement une clef d'accès ou mot de passe propre au client. Pour chaque marchand, la base de données 44 contient l'identité système du marchand ("MId"), identité reçue lors de l'abonnement au système, un compte de marchand, ou tiroir-caisse électronique ("TCE") destiné à l'encaissement des faibles montants et une identité bancaire telle que numéro de compte bancaire réel.

La figure 3 illustre schématiquement les différentes étapes d'une transaction portant sur un achat d'un bien par un client abonné à un marchand abonné. Il peut s'agir d'un bien matériel dont la livraison au client sera effectuée réellement après conclusion de la transaction ou d'un bien immatériel (tel que de l'information) qui peut être fournie au client par le réseau informatique dès le paiement électronique effectué.

#### (1) Consultation par le client

Par connexion sur le réseau "Internet" 10, un client peut consulter en ligne le catalogue ou la "vitrine" d'un marchand quelconque par accès au serveur 20 du marchand et par visualisation sur l'écran du poste client 30 des biens ou services du marchand. Sur présentation de l'identité CId du client, le serveur du marchand peut présenter au client des conditions financières particulières (par exemple une remise) applicables à la transaction éventuelle.

#### (2) Demande d'achat

Le choix du client étant arrêté sur un bien O, il est transmis au serveur du marchand sous forme d'un message contenant une identité OId du bien et l'identité CId du client. Lorsque cela est nécessaire, par exemple pour la livraison ultérieure du bien choisi, des informations complémentaires (par exemple une adresse et un horaire de livraison préféré). Cela peut être réalisé de façon commode en utilisant un formulaire électronique envoyé sur le réseau et destiné à être rempli par le client.

Dans le cas où l'achat envisagé représente un montant élevé ou est soumis à des conditions légales, une authentification préalable du client peut être souhaitée. Comme on le verra en détail plus loin l'authentification d'un client est effectuée par le serveur de paiement 40. Aussi, une demande d'authentification provenant d'un marchand est émise avantageusement sous la forme d'un ticket de paiement de valeur nulle qui est transmis au serveur de paiement par le réseau informatique via le poste client et, en cas d'authentification positive, provoque le retour d'un bon de caisse du serveur de paiement au serveur marchand, toujours via le poste client. Les procédures d'établissement d'un ticket de paiement et de renvoi d'un bon de caisse sont décrites plus en détail ci-après.

La demande d'achat émise par le client peut porter sur un seul bien ou sur plusieurs biens à fournir de façon groupée : "achat panier".

#### (3) Elaboration de la demande de paiement

En réponse à une demande d'achat, le serveur marchand élabore une demande de paiement qui peut comprendre les informations suivantes :

- Identité du marchand, ("MId");
  - Description du bien commandé, ou de chacun des biens du panier, en cas d'achats groupés;
  - Type de transaction (simple ou panier);
  - 5     - Identité du client, ("CId");
  - Identité du bien ou de l'ensemble des biens du panier, ("OId");
  - Prix de l'objet, ("Oid");
  - TVA (si applicable);
  - Date et heure de l'émission du ticket de paiement (horodatage par le
  - 10    serveur marchand);
  - Durée de validité du ticket de paiement;
  - Numéro de série dans le registre des ventes du marchand (notamment dans le cas où la transaction a comporté une étape préalable d'authentification).
- L'ensemble des informations ci-dessus est encodée dans une chaîne
- 15    d'octets qui constitue la chaîne opaque d'un ticket de paiement (ou URL de commande de bien, URL étant les initiales de "Uniform Resource Locator" ou Localisateur de Ressource Uniforme utilisé dans les logiciels WWW avec protocole HTTP), comme suit:
- URL http : < SP> < descriptif de la commande> ,
- 20    où SP est l'adresse "Internet" du serveur de paiement. Le ticket de paiement est adressé au poste client. Il est complété par deux "ancres" logiques qui permettent au client soit de l'annuler, soit de le confirmer.

#### (4) Envoi de l'ordre de paiement

- L'ordre de paiement est transmis au serveur de paiement simplement
- 25    par validation par le client de l'URL de demande de paiement. On comprendra bien que le ticket de paiement ne fait alors que transiter par le poste client.

#### (5) Emission du bon de caisse

- Sur réception d'un ordre de paiement, le serveur de paiement 40 le
- décode et procède à l'authentification du client et recherche si le paiement peut être
- 30    autorisé avant de retourner un bon de caisse ou un refus de paiement.

Les opérations d'authentification de client et d'autorisation de paiement seront décrites plus loin en détail en référence à la figure 4.

- Lorsque les vérifications effectuées ne permettent pas d'autoriser le
- paiement, une notification de refus motivée est adressée au client par le serveur de
- 35    paiement (indiquant, par exemple, compte insuffisamment approvisionné, dépassement d'un seuil autorisé pour le client, ...)



Lorsque les vérifications effectuées permettent d'autoriser le paiement, les informations contenues dans le ticket de paiement sont complétées avec un numéro de série dans le registre des transactions 45, une estampille horaire, une durée de validité (typiquement quelques dizaines de secondes) et le sceau du serveur de paiement constituant une information de certification. L'ensemble de ces informations, éventuellement après signature numérique par l'utilisation de la partie de clef privée d'un système de chiffrement à clef privée/clef publique du serveur de paiement (ce qui garantit la validité et l'intégrité de l'autorisation de paiement), est encodé dans une chaîne d'octets qui constitue la chaîne opaque d'un bon de caisse ou URL de livraison :

URL http : <M> <descriptif du bon de caisse> ,  
où <M> est l'adresse "Internet" du marchand.

#### (6) Demande de livraison

Le bon de caisse est transmis au serveur du marchand via le poste client. Ceci peut être effectué automatiquement par le logiciel implanté au poste client en utilisant la possibilité de re-routage des URL bien connue de l'homme du métier. Avant d'autoriser la livraison du bien, le serveur du marchand opère un décodage et une vérification du bon de caisse reçu. Cette vérification consiste à utiliser la clef privée éventuelle du serveur de paiement, à vérifier que la durée de validité n'est pas écoulée, et à rapprocher le contenu du bon de caisse avec celui de la demande de paiement.

#### (7) Livraison du bien

Lorsque le bon de caisse est validé par le serveur du marchand, celui-ci peut effectuer la livraison directe sur le poste client, dans le cas de bien d'information, ou adresse au poste client un document permettant le retrait du bien et précisant notamment le lieu de livraison et le nom du récipiendaire.

On notera que, dans le cas d'un achat groupé (panier), il y a création par le serveur du marchand d'un objet avec affectation d'une identité unique. Cet objet est la liste des URL de chacun des biens du panier. C'est cet objet qui est indiqué dans l'URL de commande de bien et qui permettra d'enregistrer le détail des biens achetés dans le registre de transaction du serveur de paiement.

Les figures 4A à 4C montrent les opérations effectuées par le serveur de paiement 40 en réponse à la réception d'un ordre de paiement.

Dans l'unité frontale 41 (figure 4A), l'ordre de paiement est décodé (étape 61) et sa validité est examinée (test 62) notamment du point de vue de la

durée de validité. Si le résultat de l'examen est négatif, une notification de refus est envoyée au poste client (étape 63).

Si le résultat de l'examen est positif, il est procédé ensuite à une authentification du client (étape 64), le détail de cette opération étant décrit plus loin en référence à la figure 4C. Si l'authentification est négative (test 65), une notification de refus est envoyée au client (étape 63). Si elle est positive, l'ordre de paiement (éventuellement limité à l'identité **CId** du client, à l'identité **MId** du marchand, et au prix) est transmis via la liaison 68 à l'unité dorsale 42 du serveur de paiement représenté sur la figure 2 (étape 66). La liaison 48 est une liaison sécurisée interdisant l'accès à l'unité dorsale à toute personne se connectant sur le réseau 10.

L'unité frontale 41 attend alors que l'unité dorsale décide d'autoriser ou non le paiement (étape 67). Si le paiement n'est pas autorisé, (test 68), une notification de refus est envoyée au poste client (étape 63). Si le paiement est autorisé, un bon de caisse est élaboré (étape 69), utilisant les informations enregistrées à l'étape 62. Le bon de caisse est enregistré dans une mémoire de l'unité frontale 41 (étape 70) et est adressé au serveur du marchand via le poste client (étape 71).

Au niveau de l'unité dorsale 42 (figure 4B) du serveur de paiement, à la réception d'un ordre de paiement authentifié, il est examiné si celui-ci doit être autorisé à partir du compte client **PME** via le réseau bancaire 50. A cet effet, le prix est comparé à un seuil minimum (test 72). Ce seuil est par exemple de quelques dizaines de francs.

Si le seuil est dépassé, une demande pour effectuer l'opération de paiement est lancée sur le réseau bancaire (étape 73) en utilisant l'identité bancaire correspondant à l'identité **CId** du client, telle qu'elle ressort de la consultation de la base de données 44. A la réception de la réponse positive ou négative (étape 74), celle-ci est transmise à l'unité frontale 41 (étape 75).

Si le seuil n'est pas dépassé, le paiement peut être effectué à partir du compte **PME** du client.

A cet effet, il est examiné si le compte est suffisamment approvisionné (test 76). Dans la négative, un refus d'autorisation de paiement, c'est-à-dire une réponse négative, est renvoyée à l'unité frontale (étape 75). Dans l'affirmative, le compte **PME** du client est débité du prix et le compte **TCE** de marchand correspondant à l'identité **MId** est crédité du même montant (étape 77), la transaction est inscrite dans le registre des transactions 45 (étape 78) et

l'autorisation de paiement, c'est-à-dire une réponse positive est transmise à l'unité frontale 41 avec l'indication du numéro de série de l'inscription dans le registre de transactions (étape 75).

La procédure d'authentification dans le serveur de paiement (figure 4C), à l'étape 64 de la figure 4A, comprend l'envoi au poste client, de préférence dans une forme sécurisée (chiffrée), d'une demande de clé d'accès, ou mot de passe (étape 641). A la réception sécurisée de la clé d'accès (étape 642), une comparaison est effectuée avec une information correspondante contenue dans la base de données 44 (test 643).

Si la comparaison est négative, et qu'un nombre maximum de tentatives infructueuses n'a pas été atteint (test 644), on retourne à l'étape 641. Si ce nombre maximum est atteint, l'absence d'authentification est constatée, une alerte est produite (étape 645) et une réponse négative est envoyée au poste client (étape 646). L'alerte peut consister en une annulation du compte **PME** ou en une surveillance de celui-ci afin de détecter de nouvelles tentatives d'utilisation. Si le test à l'étape 643 est positif, l'authentification est enregistrée (étape 647) et une réponse positive est élaborée (étape 648).

Des techniques de chiffrement permettant la transmission sécurisée d'informations numériques sur réseau informatique, notamment pour la demande d'envoi de clé d'accès et l'envoi de celle-ci, sont bien connues.

La procédure d'authentification décrit ici permet d'effectuer une authentification préalable d'un client dans le cas où celle-ci est nécessaire avant l'établissement d'une demande de paiement par le serveur du marchand. Pour cette authentification, il suffit alors en effet de créer un ticket de paiement dans lequel le prix indiqué est nul, comme indiqué plus haut.

L'enregistrement des bons de caisse dans l'unité frontale permet aux clients et aux marchands de procéder à des contrôles et d'en obtenir éventuellement des copies. L'enregistrement des transactions dans l'unité dorsale permet d'en conserver une trace en cas, par exemple, de contestation entre un client et un marchand.

Les comptes clients **PME** gérés par le serveur de paiement ont en principe un montant de solde plafonné et, selon le mode de réalisation préféré de l'invention, ils ne sont pas rémunérés (le système de paiement se trouvant en dehors du monde bancaire). Un réapprovisionnement de son compte **PME** par un client peut être effectué à partir de son compte bancaire, par ordre donné à son établissement bancaire.

Les comptes marchands TCE gérés par le serveur de paiement sont associés à des comptes bancaires réels des marchands dans lesquels ils sont vidés par exemple quotidiennement.

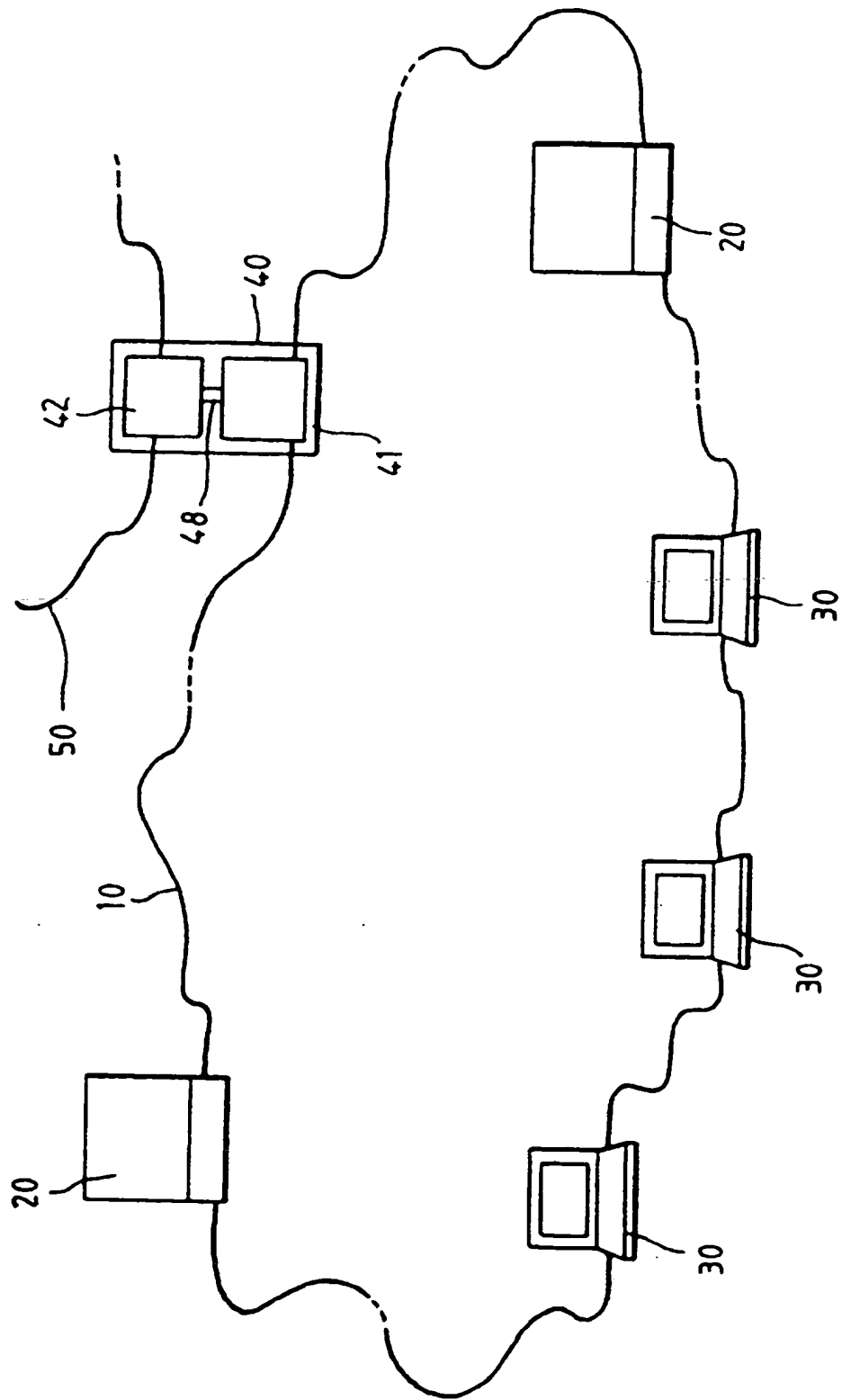
5 Bien que l'on ait décrit ci-avant un mode de mise en oeuvre d'un procédé selon l'invention dans un environnement "Internet" et avec des logiciels WWW utilisant le protocole HTTP, l'homme de l'art comprendra aisément que le  
procédé peut être mis en oeuvre avec un réseau informatique autre qu'"Internet" ou  
encore avec des logiciels serveur marchand et client n'utilisant pas le protocole  
10 HTTP de WWW. En outre des procédés d'authentification sécurisés mettant en jeu  
des dispositifs matériels tels que lecteur de carte à puce ou moyen de  
reconnaissance d'empreinte vocale pourront être prévus à la place de clefs d'accès.  
Ces dernières et d'autre modifications qui viendront à l'esprit du l'homme du métier  
sont comprises dans la philosophie et la portée de la présente invention.

### REVENDICATIONS

1. Procédé de paiement électronique pour des transactions liées à l'achat de biens offerts par des marchands à des clients via un réseau informatique ouvert sur lequel sont connectés des postes serveurs de marchands et des postes clients, caractérisé par les étapes de :
  - 5 – élaboration par un poste serveur de marchand connecté au réseau d'une demande d'autorisation de transaction, ou ticket de paiement, concernant un achat envisagé entre le marchand et un client, et comportant des informations relatives au marchand, au client, à l'objet de l'achat et à son prix,
  - 10 – transmission du ticket de paiement via le réseau informatique à un serveur de paiement distinct des postes clients et serveurs de marchands,
  - vérification automatique par le serveur de paiement si le paiement du prix est autorisé pour le client concerné, la vérification étant effectuée, selon le montant du prix à payer, soit par interrogation d'un compte client propre au client, tenu par le serveur de paiement, et destiné au paiement des petits montants, soit par  
15 interrogation sur un réseau bancaire indépendant du réseau informatique, pour les paiements de montants plus élevés,
  - si la vérification est positive, élaboration par le serveur de paiement d'une autorisation de transaction ou bon de caisse comportant au moins une partie  
20 des informations du ticket de paiement, et
  - transmission du bon de caisse au serveur de marchand via le réseau informatique, afin d'autoriser la réalisation de l'achat.
2. Procédé selon la revendication 1, caractérisé en ce que lorsqu'un bon de caisse est transmis après vérification par interrogation d'un compte client tenu  
25 par le serveur de paiement, le montant de l'achat est débité du compte client et crédité sur un compte marchand propre au marchand concerné et tenu par le serveur de paiement.
3. Procédé selon l'une quelconque des revendications 1 et 2, caractérisé en ce que la vérification par le serveur de paiement comprend une phase préalable  
30 d'authentification du client.
4. Procédé selon la revendication 3, caractérisé en ce que l'authentification est réalisée par reconnaissance d'une clef d'accès transmise par le réseau informatique du poste client au serveur de paiement.
5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en  
35 ce qu'il comprend l'élaboration par le serveur de paiement d'un bon de caisse

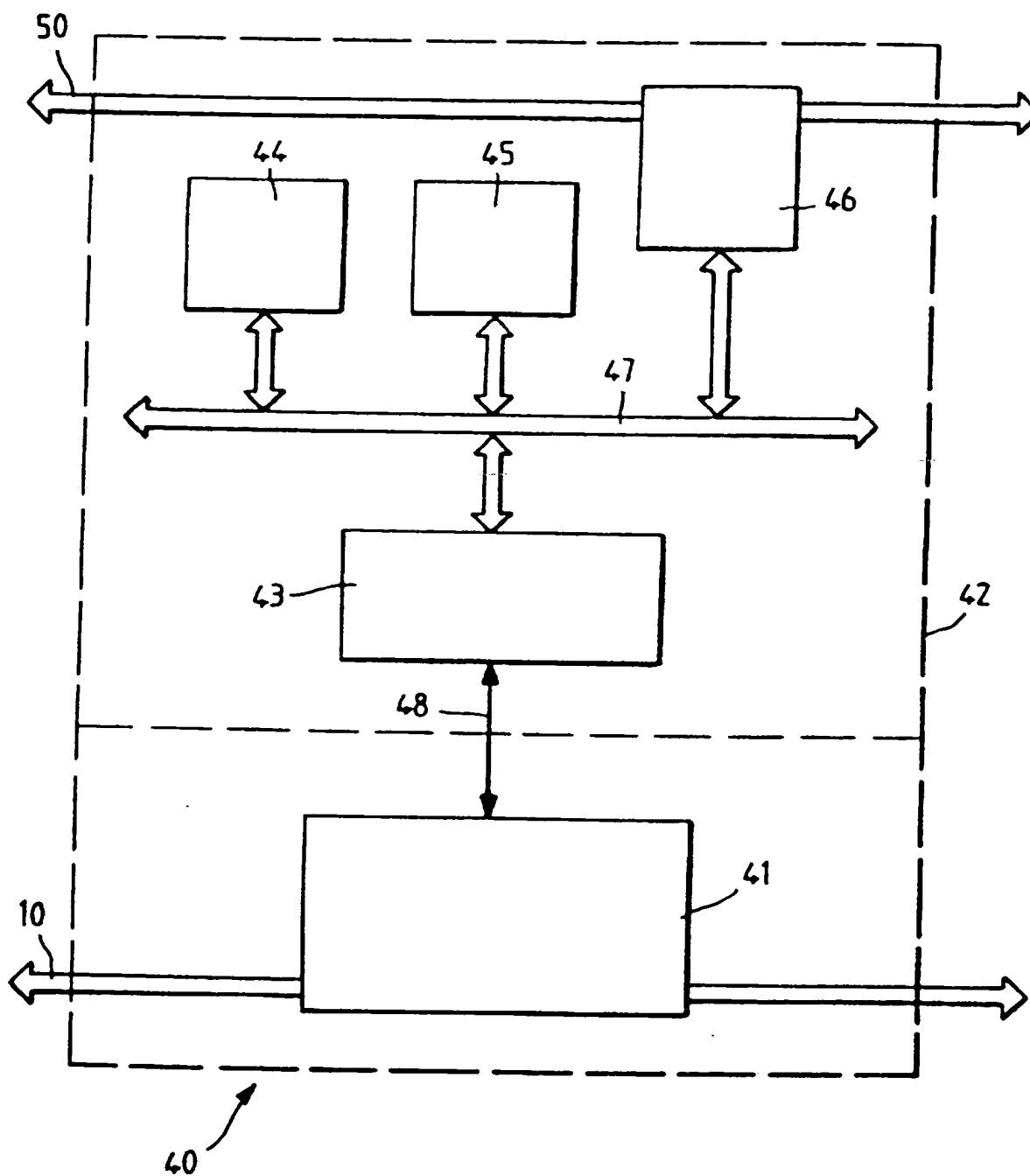
comportant au moins une partie des informations du ticket de paiement et une information de certification.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il comprend la mémorisation par le serveur de paiement des transactions autorisées, par stockage d'au moins une partie du contenu des bons de caisse.
7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que le ticket de paiement est transmis du serveur du marchand au serveur de paiement par l'intermédiaire du poste client.
8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que le bon de caisse est transmis du serveur de paiement au serveur du marchand par l'intermédiaire du poste client.
9. Système de paiement électronique pour effectuer des transactions liées à l'achat de biens offerts par des marchands à des clients via un réseau informatique ouvert, le système comportant des postes clients et des postes serveurs de marchands pouvant être connectés sur le réseau ouvert, système caractérisé en ce qu'il comporte en outre au moins un poste serveur de paiement distinct des postes clients et serveurs de marchands et comprenant :
- une unité frontale munie de moyens de connexion au réseau ouvert,
  - une unité dorsale munie de moyens de connexion à un réseau bancaire indépendant du réseau ouvert,
  - des moyens de communication entre les unités frontale et dorsale,
  - des moyens de mémorisation de comptes de clients, de comptes de fournisseurs, et
  - des moyens de traitement pour, en réponse à la réception par l'unité frontale d'une demande d'autorisation de transaction ou ticket de paiement, concernant un achat envisagé entre un marchand et un client, vérifier si le paiement du prix est autorisé pour le client concerné par interrogation du compte du client ou du réseau bancaire et, si la vérification est positive, élaborer une autorisation de transaction, ou bon de caisse afin de la transmettre sur le réseau ouvert via l'unité frontale.
10. Système de paiement selon la revendication 9, caractérisé en ce que le serveur de paiement comprend des moyens de mémorisation des transactions autorisées.



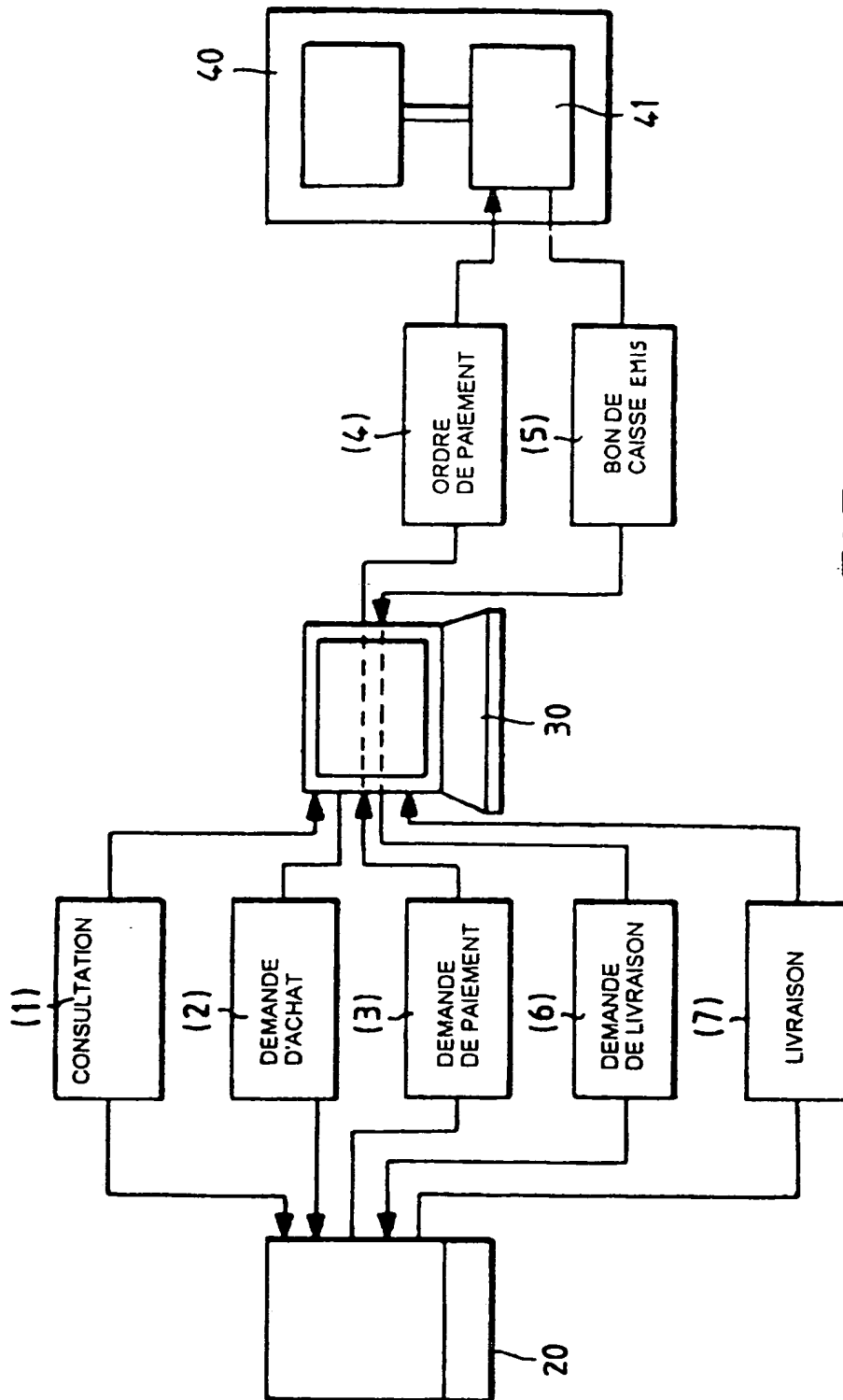
**FIG. 1**

2 / 5

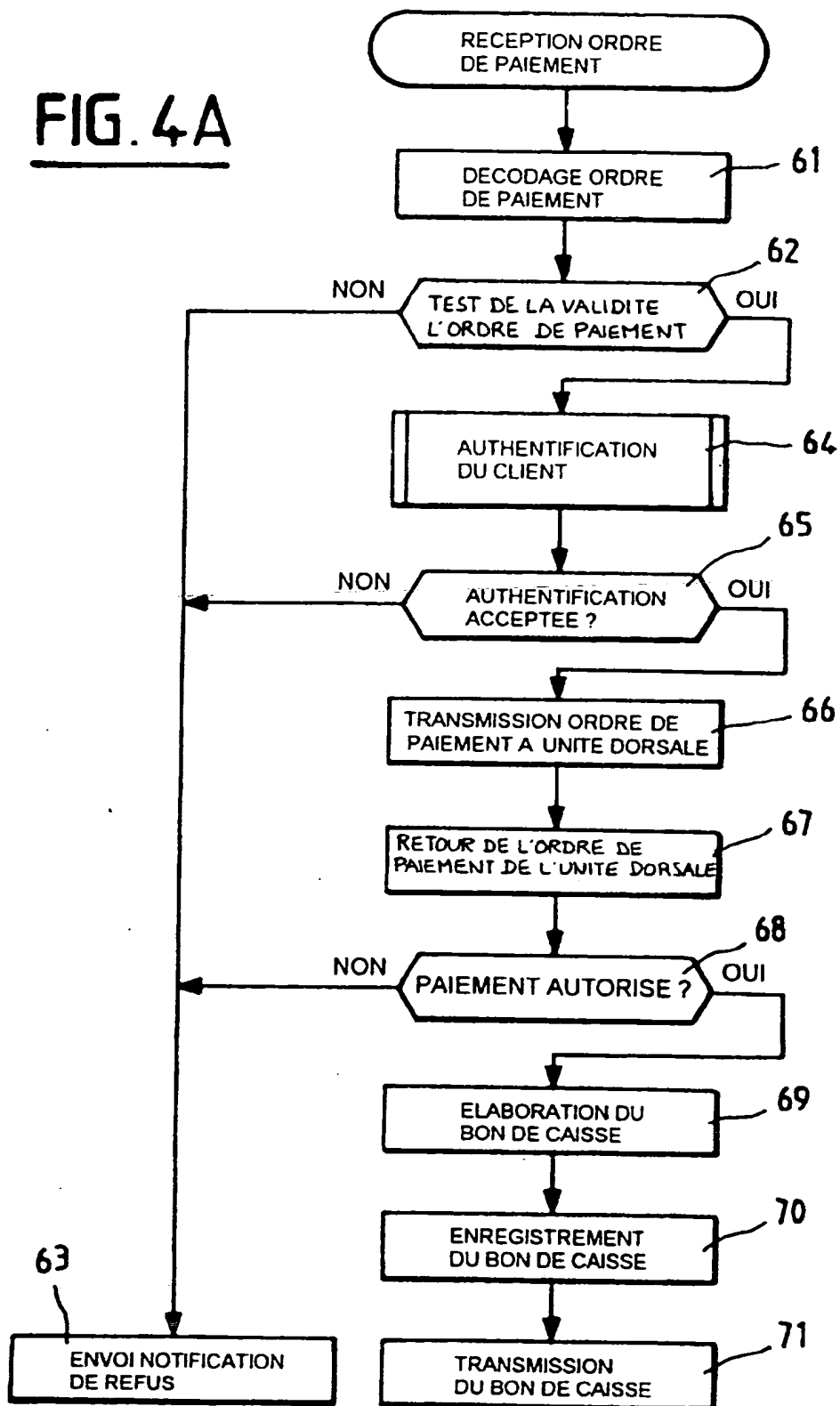
FIG. 2



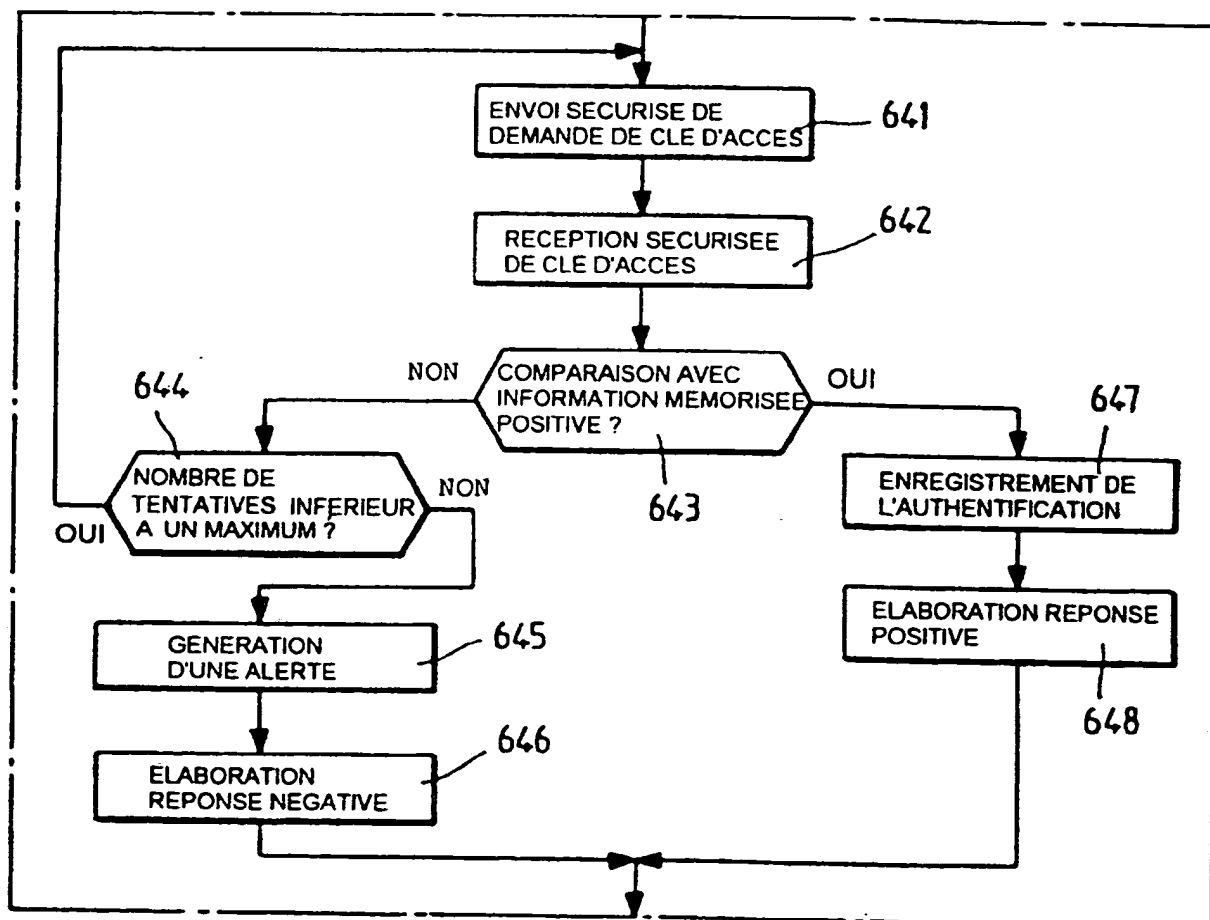
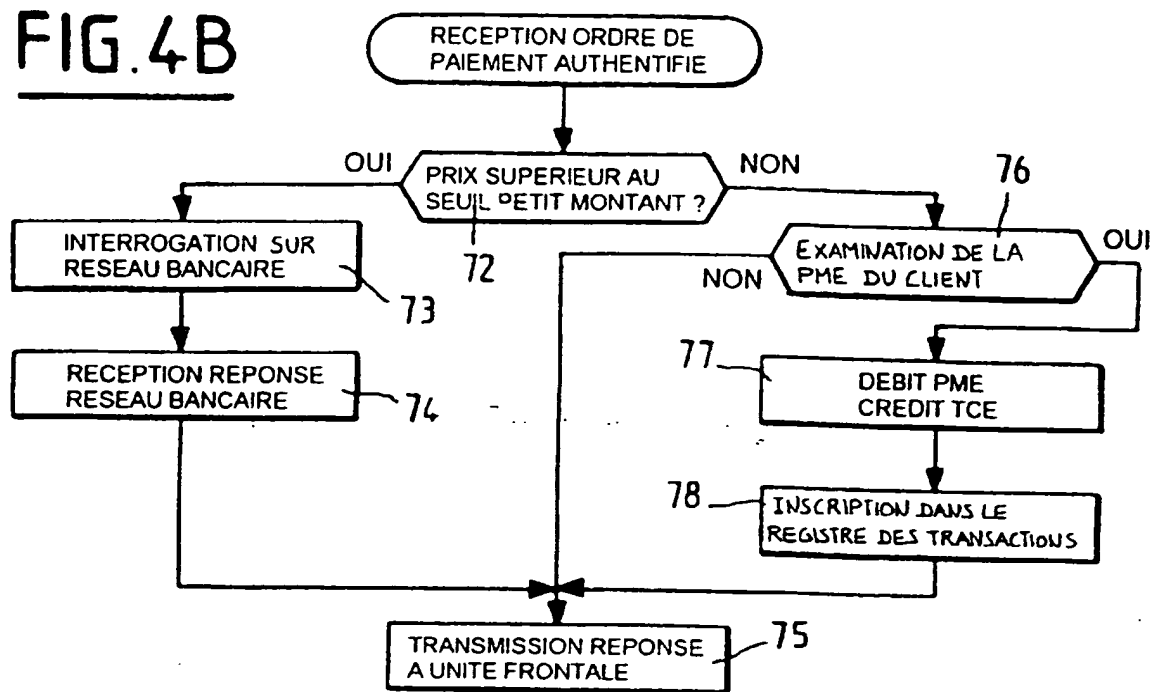
3/5

**FIG. 3**

4 / 5

FIG. 4A

5/5

**FIG. 4B****FIG. 4C**

## INTERNATIONAL SEARCH REPORT

International Application No.

PCT/FR 96/00500

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 3 852 571 A (HALL B ET AL) 3 December 1974 see column 2, line 31 - column 3, line 23 see column 10, line 19 - column 16, line 7; claims 1-8; figures 1,2 ---	1-4,6-10
A	US 5 283 829 A (ANDERSON MILTON M) 1 February 1994 see abstract; claims; figures ---	1,3,4,9
A	EP 0 501 697 A (AMERICAN TELEPHONE & TELEGRAPH) 2 September 1992 see abstract; claims 1-10 ---	1,3,6,9, 10
A	EP 0 590 861 A (AMERICAN TELEPHONE & TELEGRAPH) 6 April 1994 see the whole document ---	1,9
	-/--	

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

## \* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

\*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

\*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

\*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

\*&\* document member of the same patent family

Date of the actual completion of the international search

2 August 1996

Date of mailing of the international search report

13.08.96

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+ 31-70) 340-3016

Authorized officer

Guivol, O

# INTERNATIONAL SEARCH REPORT

Inter nal Application No  
PCT/FR 96/00500

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 258 749 A (FREER ANDREW ; SCAMELL KATZ SIEMON (GB)) 17 February 1993 ---	1
A	EP 0 359 667 A (MORS) 21 March 1990 -----	

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 96/00500

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-3852571	03-12-74	DE-A- 2058906 FR-A- 2092282 GB-A- 1293259	09-12-71 21-01-71 18-10-72
US-A-5283829	01-02-94	NONE	
EP-A-0501697	02-09-92	AU-B- 640855 AU-B- 1089692 CA-A,C 2059078 JP-A- 5095405 US-A- 5329589	02-09-93 03-09-92 28-08-92 16-04-93 12-07-94
EP-A-0590861	06-04-94	CA-A- 2100134 JP-A- 7129671 US-A- 5485510	30-03-94 19-05-95 16-01-96
GB-A-2258749	17-02-93	NONE	
EP-A-0359667	21-03-90	FR-A- 2636456 DE-T- 68908053 ES-T- 2013697	16-03-90 03-02-94 16-12-93

# RAPPORT DE RECHERCHE INTERNATIONALE

Dem Internationale No  
PCT/FR 96/00500

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**  
CIB 6 G07F/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 G07F G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 3 852 571 A (HALL B ET AL) 3 Décembre 1974 voir colonne 2, ligne 31 - colonne 3, ligne 23 voir colonne 10, ligne 19 - colonne 16, ligne 7; revendications 1-8; figures 1,2 ---	1-4,6-10
A	US 5 283 829 A (ANDERSON MILTON M) 1 Février 1994 voir abrégé; revendications; figures ---	1,3,4,9
A	EP 0 501 697 A (AMERICAN TELEPHONE & TELEGRAPH) 2 Septembre 1992 voir abrégé; revendications 1-10 ---	1,3,6,9, 10
A	EP 0 590 861 A (AMERICAN TELEPHONE & TELEGRAPH) 6 Avril 1994 voir le document en entier ---	1,9
-/--		

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

\* Catégories spéciales de documents cités:

- \*A\* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- \*E\* document antérieur, mais publié à la date de dépôt international ou après cette date
- \*L\* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- \*O\* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- \*P\* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- \*T\* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- \*X\* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- \*Y\* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- \*Z\* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

2 Août 1996

Date d'expédition du présent rapport de recherche internationale

13. 08. 96

Nom et adresse postale de l'administration chargée de la recherche internationale  
Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tél. (+ 31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+ 31-70) 340-3016

Fonctionnaire autorisé

Guivol, D

# RAPPORT DE RECHERCHE INTERNATIONALE

De le Internationale No  
PCT/FR 96/00500

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	GB 2 258 749 A (FREER ANDREW ; SCAMELL KATZ SIEMON (GB)) 17 Février 1993 ---	1
A	EP 0 359 667 A (MORS) 21 Mars 1990 -----	



# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dem . Internationale No

PCT/FR 96/00500

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US-A-3852571	03-12-74	DE-A- 2058906 FR-A- 2092282 GB-A- 1293259	09-12-71 21-01-71 18-10-72
US-A-5283829	01-02-94	AUCUN	
EP-A-0501697	02-09-92	AU-B- 640855 AU-B- 1089692 CA-A,C 2059078 JP-A- 5095405 US-A- 5329589	02-09-93 03-09-92 28-08-92 16-04-93 12-07-94
EP-A-0590861	06-04-94	CA-A- 2100134 JP-A- 7129671 US-A- 5485510	30-03-94 19-05-95 16-01-96
GB-A-2258749	17-02-93	AUCUN	
EP-A-0359667	21-03-90	FR-A- 2636456 DE-T- 68908053 ES-T- 2013697	16-03-90 03-02-94 16-12-93

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☒ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**